NOTE ON THE CLASS NUMBER OF QUADRATIC FIELDS

By L. Carlitz

1. Let d be the discriminant of the real quadratic field $R(d^{\frac{1}{2}})$ and let $h(d)$ denote the class number of the field. If p is an odd prime divisor of d, Ankeny, Artin and Chowla [1], [2] have found various expressions for the residue of $h(d)$ (mod p). In particular for $d = p$, they have stated the following theorem ([1; Theorem 4]; for proof see [4]):

$$\frac{2u}{t}h(p) \equiv \frac{A+B}{p} \pmod{p}, \tag{1.1}$$

where A is the product of the quadratic residues of p and B is the product of non-residues of p in the interval $1, p-1$; also $\epsilon = (t + up^{\frac{1}{2}})/2$ is the fundamental unit of the field ($\epsilon > 1$).

We wish to show here how (1.1) can be extended to the general case. Put

$$p_0 = (-1)^{(p-1)/2}p, \qquad d = pm = p_0 m_0\,, \qquad (m > 1), \tag{1.2}$$

and let (d/r) denote the Kronecker symbol. It follows from (1.2) that

$$\left(\frac{d}{r}\right) = \left(\frac{p_0}{r}\right)\left(\frac{m_0}{r}\right) = \left(\frac{r}{p}\right)\left(\frac{m_0}{r}\right). \tag{1.3}$$

We now put

$$A = \prod_{a=1}^{d} a^{(m_0/a)}, \qquad B = \prod_{b=1}^{d} b^{(m_0/b)}, \tag{1.4}$$

where in the first product $(a/p = 1$ while in the second $(b/p) = -1$. Replace a by $a + pr$, where now a runs through the residues of p in the interval $1, p - 1$, then

$$\begin{aligned} A &= \prod_a \prod_{r=1}^{m} (a + pr)^{(m_0/a+pr)} \\ &\equiv \prod_a a^{\sum_r (m_0/a+pr)} \equiv 1 \pmod{p}, \end{aligned}$$

since for fixed, a, $a + pr$ runs through a complete residue system (mod m). Thus $A \equiv B \equiv 1$ (mod p). We write (compare [5; Chapters 19, 20]

$$A = 1 + p\Omega, \qquad B = 1 + p\Omega'. \tag{1.5}$$

Hence

$$A^{p-1} \equiv 1 - p\Omega, \qquad B^{p-1} \equiv 1 - p\Omega' \pmod{p^2}. \tag{1.6}$$

Received May 5, 1955.